ABSTRACT OF THE DISCLOSURE

An electronic message for transmission over a network, such as the Internet, is created by encrypting a first component with a first crypto-key, which is associated with a first network entity, such that the encrypted first component can be decrypted by only the first network entity. The first crypto-key could, for example, be a symmetric crypto-key known only to the first network entity or the public non-symmetric crypto-key of a private-public non-symmetric key pair, where the private non-symmetric crypto key is known only to the first network entity. A second component, which is different than the first component, is encrypted with a second crypto-key, which is associated with a second network entity, such that the encrypted second component can also be decrypted by the first network entity. The second crypto-key could, for example, be a symmetric crypto-key known to both the first and second network entities or the private non-symmetric crypto-key of a private-public non-symmetric key pair of the second network entity, where the public non-symmetric crypto key is known to the first network entity. The encrypted first and second components are combined to create the electronic message.